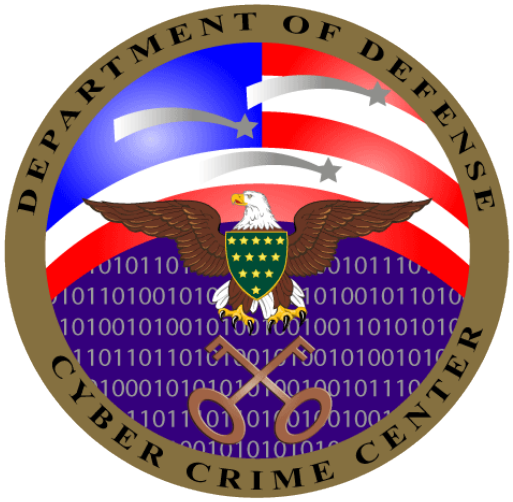


# 2011 DC3 DIGITAL FORENSICS CHALLENGE RULES
# v1.0

## 14 December 2010

# Rules Change Summary

| Section | Change Description | Date Changed |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# Table of Contents

# 1.0 INTRODUCTION

## *1.1 Background*

The Department of Defense Cyber Crime Center (DC3) sets standards for digital evidence processing, analysis, and diagnostics for any Department of Defense (DOD) investigation that requires computer forensic support to detect, enhance, or recover digital media, including audio and video. DC3 assists in criminal, counterintelligence, counterterrorism, and fraud investigations of the Defense Criminal Investigative Organizations (DCIOs) and DOD counterintelligence activities. It also supports safety investigations, the Inspector General, and commander-directed inquiries. DC3 aids in meeting intelligence community document exploitation objectives from criminal law enforcement, digital forensic, and counterintelligence perspectives. DC3 provides computer investigation training to forensic examiners, investigators, system administrators, and any other DOD members who must ensure Defense Information Systems are secure from unauthorized use, criminal and fraudulent activities, and foreign intelligence service exploitation. DC3 remains on the leading edge of computer technologies and techniques through research, development, testing, and evaluation applied to digital evidence processing and computer forensic analysis; and by partnering with governmental, academic, and private industry computer security officials.

## *1.2 Overview*

The DC3 Challenge encourages innovation from a broad range of individuals, teams, and institutions to provide technical solutions for computer forensic examiners in the lab as well as in the field. Approximately 25 different challenges ranging from basic forensics to advanced tool development are being provided to all participants. The challenges are single based challenges and are designed to be unique and separate from one another.

## *1.3 Objectives*

The objectives of the Annual Digital Forensics Challenge are to establish relationships; resolve technological issues; and develop new tools, techniques, and methodologies for the digital forensic community.

# 2.0 ELIGIBILITY CRITERIA

## *2.1 Registration*

Registration is designed to be completed online via the DC3 2011 Challenge website at http://www.dc3.mil/challenge/2011. Registration must be for all team participants in its entirety. If there is any 'anonymous' information supplied with application submittal, the application will be denied. In the unlikely event that the website is not functioning, a team member can provide the necessary information in an email to challenge@dc3.mil or call the DC3 challenge line at 410-981-6610.

## *2.2 Requirements*

Challenge entry is open to both individuals and teams. Teams may include corporate or academic entities but are not limited to these. Each entry must meet the following eligibility requirements:

- An individual cannot participate on more than one (1) team or compete with multiple entries.

- Teams will consist of one (1) to four (4) member(s).

- The team's first team member will be assigned as the team leader and considered the sole Point of Contact (POC).

- All members are required to provide their personal information (Full Name, Address, Telephone Number, Email Address, Etc) for team approval.

    - *Failure to provide accurate personal information **OR** falsifying registration information will deny your application and/or disqualify your team from challenge participation* as per Section 8.0 – Team Disqualification.

    - All changes to team members (add/update/remove) and their related information are the responsibility of team POC to update with the DC Challenge Team **in writing** to challenge@dc3.mil .

- Team and Team Member Affiliations

    - Team member affiliations are required at time of registration by the DC3 Challenge for determining team affiliation and team's potential prizes to be awarded as part of the team's approval to play in the Challenge.

    - Each team member's affiliation should be relevant to when team challenges' submissions are sent to DC3 (NOT when registered):
        - ***Civilian*** – A person or team **NOT** an academic student, in the Military, working for the Federal Government or working in the Commercial / Private Sector.
        - ***Commercial*** – A person or team that is employed for a Commercial/Private Sector representing their company. This includes contractors that work for Military, Federal, State and Local Government agencies.
        - ***Government*** – A person or team that works for their nation's Federal, State, or Local Government agency. This excludes contractors.
        - ***Military*** – A person or team that is military member or civil servant to their nation's Military.
        - ***High School Student*** – A person or team that is attending a high school as a student and has **NOT** graduated before the submission of the final Challenge package.
        - ***Undergraduate Student*** – A person or team that is attending a College/University/Technical School as a student and has **NOT** graduated before the submission of the final Challenge package.
        - ***Graduate Student*** – A person or team that is attending a graduate school as a student and has **NOT** graduated before the submission of the final Challenge package.

    - The overall team affiliation is calculated by the DC3 Challenge team based on the provided team member(s) affiliation(s).

- If a team consists of all members of the same team having the same affiliation (i.e. 4 Government members), the team will be assessed by its common member affiliation (i.e. Government.)
- If a team consists of all academic students, the highest category level will be assessed as the team affiliation. See Section 5.3 – Academic criteria for additional details.
- If a team consists of a mix of 2 or more team member affiliations that are not all academic (i.e. 2 Civilian and 1 High School Student), the team will be assessed as the team affiliation of Civilian.

o Once team affiliation is determined by the DC3 Challenge team, the team is listed under the available prize(s) based on the team's registration entry information. See Section 5.2 - Prize Eligibility for further details.

o Any changes of team member affiliation after approval to participate should be submitted to the DC3 Challenge team at challenge@dc3.mil by the POC at time of change. Be aware that changes in team members, and their affiliation, could affect the entire team affiliation as per the rules noted proceeding. Failure to report team member affiliation changes will be cause for disqualification as per Section 8.0 – Team Disqualification.

- For specific national-based prizes, all team members must be of the same citizenship category (example: U.S. or Non-U.S.) as per the prize's rules. Mixed citizenship teams consisting of U.S. and Non-U.S citizenship players will be assigned as a mixed team affiliation
- If any participant is under the age of 18 at the time of registration, the team is required to provide written authorization from a parent / legal guardian via the DC3 Permission to Participate form for **each** under-aged team member. Failure to provide this written permission will be cause for disqualification as per Section 10.0 – Team Disqualification.

- DC3 employees, current and former within the past year (2010), and their relatives are ineligible to participate for prizes; however they may compete for points only.

# 3.0 PRIZE SPONSORSHIPS

The following groups are sponsoring prizes for categories of winners of the 2011 DC3 Challenge:

- Department of Defense Cyber Crime Center (DC3)
- The SysAdmin, Audit, Network, Security (SANS) Institute
- International Multilateral Partnership Against Cyber-Threats (IMPACT)
- International Council of Electronic Commerce Consultants (EC-Council)
- Johns Hopkins University Carey Business School (JHU) CyberWatch (CW)
- Cyber Security Challenge United Kingdom (UK)

.

## 3.1 SANS Institute

The SysAdmin, Audit, Network, Security (SANS) Institute is one of the most trusted and by far the largest source for information security training and certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system - Internet Storm Center. SANS is also a sponsor in the U.S. Cyber Challenge, ran by the Center for Strategic & International Studies (CSIS).

## 3.2 IMPACT

The International Multilateral Partnership Against Cyber-Threats (IMPACT) is the first global public-private initiative against cyber-terrorism. IMPACT is dedicated to bringing together governments, industry leaders and cyber security experts to enhance the global community's capacity to prevent defend and respond to cyber threats. IMPACT and DC3 have partnered to provide a Digital Forensic Challenge opportunity for non-U.S. entries. This opportunity will provide an international aspect to a previously U.S.-based event and allow additional insight into global methods to fight cyber crime.

## 3.3 EC-Council

The International Council of Electronic Commerce Consultants (EC-Council) is a world leader in Information Security Certification and Training. With over 450 training locations of its information security courses in over 60 countries, it is the undisputed world leader in technical training and certification for the Information Security community. It is the most trusted source for vendor neutral Information Security training solution. EC-Council and DC3 have partnered to provide a Digital Forensic Challenge opportunity for both U.S. Government and U.S. Military team prizes along with Civilian and Commercial teams for all U.S. and non-U.S. entries. This opportunity will provide additional prizes for winners in these categories for continuing education in the information security field.

## 3.4 John Hopkins University/CyberWatch (JHU/CW)

With a history of educating business leaders since 1916, the Johns Hopkins University Carey Business School (JHU) specializes in creating innovative programs that anticipate and reflect global business trends. The School also draws upon the strengths of other Johns Hopkins schools, including the Johns Hopkins Bloomberg School of Public Health, the School of Medicine, School of Nursing, the Whiting School of Engineering, and the Zanvyl Krieger School of Arts and Sciences.

CyberWatch (CW) is a consortium of higher education institutions, businesses, and government agencies focused on building and maintaining a stronger information assurance workforce. Consortium participants collaborate to share best practices, methodologies, curricula, and course modules and materials. It is an Advanced Technological Education (ATE) Center, headquartered at Prince George's Community College, and funded by a grant from the National Science Foundation (NSF). The CyberWatch goals are focused on information assurance (IA) education at all levels, from elementary through graduate school, but especially the community college level, and include curriculum development, faculty professional development, student development, career pathways, and public awareness.

## 3.5 Cyber Security Challenge UK (UK Challenge)

Cyber Security Challenge UK is a program of national challenges, designed by experts, to identify and nurture the UK's future cyber security workforce. Established by a management

consortium of key figures in cyber security, it will test the nation's cyber skills, excite and inspire entrants to develop their talents, and clarify and enable pathways to the increasingly challenging and diverse range of cyber security jobs.

# 4.0 THE CHALLENGE

## *4.1 Challenge Objectives*

The Objectives of the Annual Digital Forensics Challenge are to:

- Establish relationships within the Digital Forensics Community;
- Resolve issues facing the Digital Forensics Community;
- Develop new tools, techniques, and methodologies for the Digital Forensic Community

## *4.2 Challenge Rules*

The Challenge Rules are published on the DC3 Challenge Website (www.dc3.mil/challenge) and are subject to change. All changes will be documented as they occur. Please review and refer back on a regular basis to ensure that compliance in all areas is maintained.

## *4.3 Challenge Grading*

There are 23 single scenario based problem challenges. The chart of each specific challenge and corresponding points can be found in the Appendix under A-2 Challenges and Point Structure. There are five (5) 100 point challenges, four (4) 200 point challenges, four (4) 300 point challenges, three (3) 400 point challenges, and seven (7) 500 point challenges.

## *4.4 Challenge Bonus Points*

A team may acquire additional bonus points for early challenge submissions to the DC3 Challenge. The solution submitted for each challenge scenario is eligible for the bonus award based on the time it is submitted to DC3 Challenge. Only the team's initial submission is eligible for a bonus award points.

Bonus points are calculated based on the team's grade for that Challenge submission and the submission date. The team's initial submission is the **FINAL** submission for that specific Challenge.

Bonus points will be awarded based on the following schedule:

| Date Range | Bonus Awarded to Challenge Score |
|---|---|
| **15 Dec 2010 -- 1 May 2011** | 20% |
| **2 May 2011 -- 1 July 2011** | 10% |
| **2 July 2011 -- 1 Oct 2011** | 5% |
| **2 Oct 2011 -- 1 Nov 2011** | 0% |

Example:

- Team A submits their Challenge 101 submission on 1 Feb 2011.
- DC3 grades Team A's Challenge 101 submission after 1 May 2011.
  - Their submission is graded by DC3 at 90 out of 100 points.
  - Their submission is marked at 20% bonus points due to their 1 Feb 2011 submission date.
- Team A is awarded the following points for Challenge 101:
  90 points graded + (90 pts * 20%) bonus = 108 points total

## *4.5 Challenge Schedule / Key Dates*

- **4 Dec 2010 – Announcement of DC3 Challenge 2011**

- **15 Dec 2010 - Registration Begins**
  - Registration and Challenge packets containing all of the challenge materials will be available for download only on or about 15 December 2010.
  - Applications received each day by close of business (COB) will be processed within 1-3 business days for approval.

- **26 Jan 2011 – Official announcement** at the 2011 DC3 Cyber Crime Conference, Atlanta, GA

- **1 May 2011 – Last day for 20% Bonus points**

- **1 July 2011 – Last day for 10% Bonus points**

- **1 Oct 2011 – Last day for 5% Bonus points**

- **1 Nov 2011 - Registration Ends**
  - Registrations are no longer accepted to the Challenge 2011.

- **2 Nov 2011 – Submission Entry Deadline**
  - All Challenge 2011 solutions, including scripts and non-commercial programs created by the team, must be uploaded or postmarked to DC3 no later than November 1st, 2011 at 11:59:59 PM EST to be eligible for a prize in their assigned category.
  - Challenge solutions received after 1 November 2011 EST will not be accepted for prizes. Scoring after this date will be at the discretion of DC3.

- **1 Dec 2011 – DC3 Challenge Winners Announced**
  - All participants will be notified via email of the posting of Challenge scoring results to the DC3 Challenge Website.
  - Final results will be posted on the DC3 Challenge Website.
  - In the event of a tie score for the top challenge solution package, the tie will be broken by the time difference between INITIAL download of challenge packet and LAST individual Challenge submittal (by electronic upload or postmarked date) of the team's solution packets.

# 5.0 PRIZE CRITERIA

## *5.1 Prizes*

Based upon their team affiliation criteria, several prizes are available to Challenge teams based on their team's eligibility per prize provided by the DC3 Challenge sponsor's requirements.

Each member of the winning team will also receive a plaque as well as formal recognition at the conference by DC3.

## *5.2 Prize Eligibility*

### 5.2.1 DC3 Prize Requirements

The winning teams of the Civilian, Corporate / Private Sector, Federal Government, Military, or Academic student categories will receive a trip to the 2011 DoD Cyber Crime Conference by DC3, based on government per Diem (airfare, lodging, meals, and paid conference fees) for up to 4 members.

Additional prize eligibility requirements are as follows:

- All team members must hold U.S. citizenship.
- All team members must be able to travel from within the Continental United States in order to claim the trip to the Conference (U.S. citizens abroad are eligible providing they transport themselves to the Continental United States.)
- All team members must meet all other previously stated Challenge Rules and Requirements.
- Any team or team member(s) under the age of 18 must provide written permission to participate in the challenge.

### 5.2.2 SANS Prize Requirements

The winning teams of the High School, Undergraduate, and Graduate student academic categories will receive a trip to the 2011 DoD Cyber Crime Conference by SANS.

- All team members must hold U.S. citizenship.
- All team members are actively attending as a U.S. student at a U.S. High School, U.S. Undergraduate or U.S. Graduate College upon submission of your results as per the Academic Criteria in Section 5.3.
- Be able to travel from within the Continental United States in order to claim the trip to the Conference (U.S. citizens abroad are eligible providing they transport themselves to the Continental United States).
- All team members must meet all other previously stated requirements of the Challenge Rules.

### 5.2.3 IMPACT Prize Requirements

The Non-U.S. citizen winner(s) of the International category from an IMPACT-member country will be eligible to fly to Malaysia for a tour of the IMPACT facility in Cyberjaya. They will be officially presented with a commemorative plaque and potential grants of EC-Council and SANS courses. The results of the IMPACT/DC3

Challenge winner will be given honorable mention at the Department of Defense Cyber Conference in January 2011, and published for community utilization.

In addition to the DC3 team requirements, the below are additional IMPACT requirements:

- All team participants DO NOT hold U.S. citizenship.
- All team members' legal residences are located outside of the U.S. *AND* in an IMPACT member country (any country listed on the following website: http://www.itu.int/cgi-bin/htsh/mm/scripts/mm.list?_search=ITUstates )
- All team members must meet all other non-U.S. Challenge Rules and Requirements.
- All current DC3 or IMPACT personnel and former DC3 or IMPACT personnel who are within one calendar year (1 Jan 2010) are ineligible to participate.

For more information on IMPACT participation requirements, visit the IMPACT website at www.impact-alliance.org under events / upcoming / IMPACT/DC3 Challenge.

### 5.2.4 EC-Council Prize Requirements

The winning teams of the Civilian, Commercial, Government, and Military categories will receive the following prizes for up to 4 members from the EC-Council:

a. A Plaque
b. A Pass to the Hacker Halted Conference worth $1799
c. Any free EC-Council electronic courseware of choice for the winners on Ethical Hacking, Computer Forensic, Security Analysis or Disaster Recovery worth $650 each

Civilian and Commercial team prize eligibility requirements

- Prizes will be awarded for teams in the Civilian and Commercial categories
- Team members may consists of U.S. and/or non-U.S. citizens

Government and Military team prize eligibility requirements

- Prizes will be awarded for teams in the Government and Military categories
- Team members must hold U.S. citizenship.

Additional prize eligibility requirements are as follows:

- All team members are responsible for travel arrangements and costs
- Any team or team member(s) under the age of 18 must provide written permission to participate in the challenge.
- Meet all other Challenge Rules requirements.

### 5.2.5 John Hopkins University / CyberWatch (JHU/CW) Prize Requirements

Johns Hopkins University Carey Business School, CyberWatch, and DC3 have partnered together to provide an opportunity for High School and Undergraduate Student teams attending U.S. Community Colleges (2 year institutions).

The Johns Hopkins University/CyberWatch (JHU/CW) winning team will be recognized as the academic leader at the U.S. Community College level. The

winning team members will also be presented with an award to mark their outstanding achievement.

In addition to the DC3 team requirements, the below are additional JHU/CW requirements:

- All team members must provide their U.S. Community College they are attending in their team's application form
- All team members must be actively attending a U.S. Community College at the time of their submission as High School Students and/or Undergraduate Students
- Team members may consist of U.S. and/non-U.S. citizens
- Any team or team member(s) under the age of 18 must provide written permission (from parent or guardian) to participate in the challenge
- Meet all other and academic Challenge Rules requirements.

### 5.2.6 UK Challenge Prize Requirements

Cyber Security Challenge UK and DC3 have partnered together to provide an opportunity for teams consisting of all UK citizens residing in the UK.

The UK Challenge winning team will be offered two prizes from Cyber Security Challenge UK:

- Two weeks at the new UK Cyber Security Academy, which develops the skills required of next-generation cyber security specialists, including courses on digital forensics, threat and risk management, cyber-crime, and emerging security technologies.
- Invitations to take part in the Cyber Security Challenge UK's masterclass challenge to compete against other successful contestants from other UK Challenge competitions

In addition to the DC3 team requirements, the below are additional UK Challenge requirements:

- Team members must be UK citizens only and must have primary residency in the UK. Teams of mixed citizenship do not qualify for this prize.
- Teams must also be registered at the UK Challenge website at https://cybersecuritychallenge.org.uk/candidates/registration.html
- Any team or team member(s) under the age of 18 must provide written permission (from parent or guardian) to participate in the challenge.
- Meet all other Challenge Rules requirements.

## *5.3 Academic Criteria*

Should an academic category be selected as a team category, the following applies:

- Team member must be enrolled and in good standing for the academic institution attending ON the date you submit your solutions package to be eligible for placement in the Academic category.
  - Proof of enrollment and student status by the Academic Institution ("Full-time", "Part-time") must be provided
  - A letter or fax on the institution letterhead, signed by team member and institution administrative office will suffice
  - Age of the player on the date of the Challenge solution is submitted does not matter

- Failure to provide proof of enrollment with appropriate signatures will disqualify the team from the Academic category and will be placed in the Civilian / Private Sector category.

- If the team consists of students from different academic categories (e.g. 2 high school students, 1 undergraduate student, and 1 graduate student), the highest academic category level will be used to assess the category status for the team. In the example above, the team's category would be designated as Graduate students.

### 5.3.1 Graduate

- Individuals / Team status **will be** placed in the **Graduate (PG)** category if they are still in a Graduate school on the date when the Challenge 2011 package **is submitted** (*not when you apply*).
- PG team (s) who submits their package **prior** to graduating will be placed in the PG category.
- PG team (s) who submits their package **after** graduating will be placed in the category of Military, Federal Government, or Commercial/Private Sector and are ineligible for Academic recognition.
- Should the Individual / Team member have a change in their expected graduation date, they **must** inform the DC3 Challenge staff (i.e. anticipated Graduation Aug 2011 changes to Dec 2011 – status will remain in the PG category). Proof of this change will have to be provided.

### 5.3.2 Undergraduate

- Individuals /Team status **will be** placed in the **Undergraduate (UG)** category if they are still in an Undergraduate program on the date when the Challenge 2011 package **is submitted** (*not when you apply*).
- UG team (s) who submits their package **prior** to graduating will be placed in the UG category.
- UG team (s) who submits their package **after** graduating but while attending a graduate program will be placed in the PG category.
- UG person(s) who submits their package **after** graduating but **not** attending a graduate program will be placed in the category of Military, Federal Government, Commercial/Private, or Civilian and will be ineligible for Academic recognition.

### 5.3.3 High School

- Individuals / Teams **will be** placed in the **High School (HS)** category on the date when the Challenge 2011 package **is submitted** (*not when you apply*).
- HS senior(s) or Team with a HS senior member who submits their package **prior** to graduating will be placed in the HS category.
- HS senior(s) or Team with a HS senior member who submits their package **after** graduating, but while attending college/university/technical program will be placed in the Undergraduate (UG) category.
- HS senior(s) or Team with a HS senior member who submits their package **after** graduating, but **not** attending college/university/technical program will be placed in the category of Military, Federal Government, Commercial/Private, or Civilian and will be ineligible for Academic recognition.

## *5.4 Judging and Challenge Rules*

Challenge Judges will adjudicate and resolve any discrepancies throughout the grading process. In the event of a tie for equal points, the team providing the challenge submissions with the shortest amount of time (based on the difference of the time between the INITIAL challenge approval email and the LAST team submission to the DC3) will be declared as the winner. **All decisions of the DC3 Challenge Judges are final**.

### 5.4.1 Methods to Submit Solutions

Team submission packages can be submitted to DC3 via two ways:

- *By single packages for each Individual Challenge submitted over time* ***(RECOMMENDED)***
  Uploading individual Challenge submissions via electronic submission only, including tools and scripts. This allows teams to submit individual Challenges as they are completed to DC3 before the Submission deadline.

- *By a complete package of all Challenge solutions at submitted one time*
  Via electronic submission or mailed to DC3 before the deadlines stated in Section 4.5 - Challenge Schedule / Key Dates in the DC3 Challenge rules

### 5.4.2 Terms of Submitting Solutions

By submitting a proposed solution to the DC3 Challenge, you agree to the following terms:

- For each tool (software, script, and method/technique) used in your Challenge solutions, it is documented in each individual Challenge as per Section 5.4.3 – Terms of Submitting Tools Used in Solving Challenges
- All submissions (individual challenges and packages) to DC3 are considered final and no revisions are allowed unless authorized by DC3.

  ***Example:*** If one individual Challenge is uploaded on Oct 01st, 2011 and the same individual Challenge is uploaded on Oct 10th 2011 for the same Challenge, the first submission only will be graded.

- Teams are responsible for verifying their submissions are accurate before providing to DC3.
- If a team has provided their submission in error, they must contact the DC3 Challenge team at challenge@dc3.mil within 2 business days of their submission to remove it from challenge grading.
- Solutions and answers must been checked for viruses, trojans, and malicious code using commercially available antivirus software and certify that it is free of those malicious computer programs.
- DC3 is the final arbiter of any dispute concerning interpretation of the rules for the DC3 Challenge. **ALL DECISIONS ARE FINAL.**

### 5.4.3 Terms of Submitting Tools Used in Solving Challenges

For each tool (program, script, and method/technique) used toward Challenge solutions, the following information must be provided with each Challenge solution - failure to provide can disqualify a team as per Section 8.0 – Team Disqualification:

- **Custom Developed tools (including Level 500 tools)**
  This includes all non-commercial tools OR modified open-source tools used in all Challenges. All Level 500 tools are considered this type of tool – **NO EXCEPTIONS**.
  - Documentation
    - Step by step instructions, to include "screen shots" as appropriate on how to use the tool
    - For level 500 tools, include additional documentation:
      - Include documentation and screenshots of your results of your validation of the Challenge against your test bed.
      - A completed test plan outlining the steps necessary for a functional test (template is provide within the Level 500 Challenges)
      - A completed Tool Evaluation Worksheet form that includes your tool's information, dependencies, and test bed information.
  - Tool
    - A copy of each non-commercial tool and/or script OR modified open-source tools and/or scripts used to accomplish the Challenge solution(s).
    - For level 500 tools, include addition data:
      - Data test case used to validate your tool.
      - Listing of execution dependencies in the Tool Evaluation Worksheet

- **Resubmission of Custom Developed tools**
  This includes all tools developed for past DC3 Challenge solutions re-used or improved for the 2011 DC3 Challenge.
  - Include all requirements listed in "Custom Developed tools"
  - Additional requirements:
    - A list of changes of the tool that documents improvements, increased functionality, etc to be awarded full points.
    - Submission of tools if submitted "as-is" from the prior year's Challenge without any form of improvement, will receive zero points.

- **Commercial tools**
  This includes all commercial tools AND closed-source tools for all Challenge solutions except Level 500 tools.
  - Name of the tool and version
  - Tool's company
  - A URL to the company's website

- **Open Source tools**
  This includes all tools with source code shared to the public Internet not used in Level 500 Challenge solutions.
  - Name of the tool
  - A URL to the site from the open source sharing site must be provided. Examples of the open source sharing sites include Source Forge, Google Code, Code Plex, etc.

# 6.0 INTELLECTUAL PROPERTY

All tools and methods created by the Challenge participants will remain the intellectual property of the creator(s). DC3 reserves the right to copy all tools, scripts, and methods/techniques for our independent testing and validation. Failure to provide the required tools, scripts, and methods / techniques upon request will disqualify the team from the DC3 Challenge participation.

All team submissions with team-created tools, techniques, solutions, and responses, in their entirety, may be shared, in their entirety, with the Challenge participants, DOD partners, and the digital forensics community . These tools, techniques, solutions, and responses may be documented and publicized in addition with the general public at DC3's discretion.

**It is recommended that all teams double-check their Challenge submissions to remove any possible personal identifiable data you are not willing to release to the public. It is not the responsibility of DC3 to remove this data.**

# 7.0 LIMITATION OF LIABILITY

The computer data and media supplied for the DC3 Challenge has been checked for computer viruses, Trojans, and other malicious code using commercial antivirus software configured with current signatures as of December 15th, 2010 and is found to be free of such programs. If the materials received appear tampered with discontinue use immediately and return the materials to DC3.

In consideration of participating in the DC3 challenge, contestants acknowledge that DC3 is not responsible for any damage caused to any computer or network due to the loading of, or operation of the storage media holding the DC3 Challenge materials.

# 8.0 TEAM DISQUALIFICATION

Registered individuals/teams will be disqualified for any of the following reasons:

- Failure to provide accurate personal information and/or falsifying registration information
- Failure to provide scripts, programs, and/or methods as referenced in Section 5.4.3 -- Terms of Submitting Tools Used in Solving Challenges in the DC3 Challenge Rules
- If at the time of submission grading and verification, it is determined that a team or member of a team has not met the eligibility requirements, the entire team shall be terminated without regard to Challenge performance in meeting prize objectives
- Failure to submit documents by the required solution due date
- Fraudulent acts, statements, or misrepresentations involving any DC3 or other federal government documentation or systems used for the challenge.
- Violation of any federal, state, or local law or regulation determined to be inconsistent with the DC3 Challenge.
- Any team member under the age of 18 must submit a DC3 Permission to Participate form, signed by a parent / legal guardian to participate in the Challenge. If, it is discovered that a team member is under the age of 18 and has not submitted this form, the team will be immediately disqualified.

# 9.0 CHALLENGE CANCELLATION

The DC3 reserves the right to cancel this challenge at any time leading up and during the Challenge time frame.

# 10.0 PRIVACY POLICY

All Team information provided during team registration for the DC3 Challenge is collected for the following purposes:

- Vetting and approval of teams to play in the DC3 Challenge
- Determine the team's available prizes from DC3 Challenge sponsors as stated in Section 5.0 – Prize Criteria
- Statistical reporting of the DC3 Challenge to the public and Challenge sponsors/partners
- Contacting teams to provide:
    - News and updates about the DC3 Challenge
    - Opportunities related to the DC3 Challenge and other government/academic Cyber Challenges
    - Verification of winners and award prizes with DC3 Challenge sponsors

## *10.1 DOD Privacy Act Statement*

DC3 Challenge will only share the information you give us with another government agency if your inquiry relates to that agency, or as otherwise required by law. DC3 Challenge never collects information for commercial marketing.

## *10.2 Contact Purposes*

DC3 Challenge will remain the primary contact for any request for contact information for Challenge teams during the Challenge process. These requests will be routed by DC3 Challenge to the Challenge team leader for approval for release. It is the Challenge team's discretion to be contacted by the interested party outside of DC3 thereafter.

For DC3 Challenge news and updates, teams may elect to "opt-out" by contacting the DC3 Challenge team at challenge@dc3.mil

## *10.3 Statistical Purposes*

For DC3 Challenge and other government/academic Cyber Challenge promotional purposes, specific anonymous information may be shared with 3rd parties. This information will be unassociated from Team Names and their Team Member's personal and contact information. This information includes the following:

- Member affiliations, states, and countries from Team Members as part of the statistical reporting of the DC3 Challenge's progress with the public and press.
- Member affiliations, U.S. citizenship, schools, states, zip codes, and countries from Team Members may be shared with the DC3 Challenge sponsors/partners and other partners as part of government/academic Cyber Challenges.

# APPENDIX

## *A-1: Challenges and Point Structure*

| Points | Challenge Title |
|---|---|
| 100 | Windows Registry Analysis |
| 100 | File Hash Identification |
| 100 | File Signature Analysis |
| 100 | Creation of Affidavit for Search Seizure Warrant |
| 100 | Hot Spot Surveillance |
| 200 | File Data Examination |
| 200 | Steganography Level 2 |
| 200 | Password Cracking |
| 200 | VMWare Memory Analysis |
| 300 | Network Trap and Trace |
| 300 | Encrypted Device Image |
| 300 | Shadow Volume Win7 Registry Analysis |
| 300 | Unallocated File Recovery |
| 400 | Shadow Volumes Analysis |
| 400 | Steganography Level 4 |
| 400 | Encrypted Drive Recovery |
| 500 | Language Identifier and Translator Tool Development |
| 500 | Imaging the Android OS Tool Development |
| 500 | MFT File Reader |
| 500 | Text String Searching Tool Development |
| 500 | Data Recovery from HPA as a Universal Tool or per Manufacturer Tool Development |
| 500 | Data Recovery from Unmarried TPM Hard Disk Tool Development |
| 500 | VSC Parser Tool Development |